Statewide Information Technology

STATE OF NORTH CAROLINA
George Bakolia, State CIO

STATEWIDE SECURITY MANUAL CONVERSION TABLE
OLD POLICIES/STANDARDS TO NEW STANDARDS

The following chart sets forth the old security policies and standards and the cross references to the new security standards. It also lists those security policies/standards that will remain in place. As the new security standards are approved, the old policies and standards that are being replaced will be removed from the web pages.

OLD POLICY/STANDARD	CROSS REFERENCES TO NEW STANDARDS
Information Asset Protection	010101 – Defining Information 010103 – Storing and Handling Classified Information 020121 – Acceptable Usage of Information Assets
Use of the State Network (Acceptable Use Policy)	030303 – Sending Electronic Mail 020121 – Acceptable Usage of Information Assets 100301 – Using the Internet in an Acceptable Way 030312 – Using the Internet for Work Purposes
Policy and Guidelines for Data Handling	010103 – Storing and Handling Classified Information 010104 – Isolating Top Secret Information 010105 – Classifying Information 010106 – Accepting Ownership for Classified Information
Identification and Authentication Using IDs and Passwords	020106 – Managing Passwords 050706 – Logon and Logoff from your Computer 100302 – Keeping Passwords/PIN Numbers Confidential
Public Key Infrastructure and Digital Certificates	030302 – Using and Receiving Digital Signatures
Policy and Guidelines for Developing Privacy Policies for Users of State Information Systems	120106 – Legal Safeguards against Computer Misuse
Application Security Policy With Guidelines	This policy remains as written and is located under Other Security Standards and Policies.
Policy and Guidelines for Developing Privacy	This policy remains as written and is located under Privacy.

Policies for Private Citizens Using State Information Systems	
Policy and Guidelines for Developing Filtering and Monitoring Policies for State Employees and Third Party Contractors Using State Information Systems	This policy remains as written and is located under Privacy.
Information Technology Business Continuity Management Policy	Chapter 14
Enterprise Authentication and Authorization Services Policy	This policy remains as written and is located under Other Security Standards and Policies.
Virus Protection Policy and Guidelines	060109 – Defending Against Virus Attacks 060110 – Responding to Virus Incidents 060111 – Installing Virus Scanning Software
Notification Banner Policy and Guidelines	120106 – Legal Safeguards against Computer Misuse. *See also*, privacy.
E-Mail Notification Policy	This policy remains as written and is located under Privacy.
Policy and Guidelines on Confidential Information Technology Security Records Provided to State CIO	This policy remains as written and is located under Other Security Standards and Policies.
Network Security Policy	030108 – Network Security
Information Technology Risk Management with Guidelines	This policy remains as written and is located under Other Security Standards and Policies.
Remote Access Policy, including Mobile Computing and Telecommuting	020112 – Controlling Remote User Access 030103 – Accessing Your Network Remotely 050404 – Working from Home or Other Off-Site Location (Teleworking)
Incident Management	060102 – Minimizing the Impact of Cyber Attacks 060103 – Collecting Evidence for Cyber Crime Prosecution 060108 – Handling Hoax Virus Warnings 060110 – Responding to Virus Incidents 120401 – Recording Evidence of information Security Incidents Chapter 13 – Detecting and Responding to IS Incidents
DNS Enterprise Security Standard	This standard remains as written and is located under Other Security Standards and

	Policies.
User ID and Password Standard	020106 – Managing Passwords 050403 – Using Laptop/Portable Computers 100302 – Keeping Passwords/PIN Numbers Confidential
Permanent Removal of Data from Electronic Media Standard	030903 – Using External Disposal Firms 040301 – Disposing of Software 050701 – Disposing of Obsolete Equipment
Desktop and Laptop Security Standard	020103 – Securing Unattended Work Stations 020106 – Managing Passwords 030902 – Loading Personal Screensavers 050402 – Issuing Laptop/Portable Computers to Personnel 050403 – Using Laptop/Portable Computers 050408 – Day to Day Use of Laptop/Portable Computers 050705 – Clear Screen 050706 – Logon and Logoff from your Computer
Wireless Network Access Security Standard	090301 – Electronic Eavesdropping
Vulnerability Management Standard	040106 – Technical Vulnerability Management
Security Framework Standard	020115 – Access Control Framework
Remote Access Security Standard	020112 – Controlling Remote User Access 030103 – Accessing Your Network Remotely
Incident Response Standard	120401- Recording Evidence of Information Security Incidents
Firewall Configuration Security Standard	This standard remains as written and is located under Other Security Standards and Policies.
Electronic Mail Server Security Standard	This standard remains as written and is located under Other Security Standards and Policies.